

AFFIDAVIT

I, Juan Carlos Razon, being first duly Sworn, hereby depose and state as follows:

INTRODUCTION

1. This affidavit is also made in support of an Application for a Search Warrant for the following properties, their common areas, and appurtenances, for the evidence described in Attachment B:

- a. **MICHAEL SELLERS's** residence at 47 Huxley Street, Providence, Rhode Island 02920 ("TARGET PREMISES"), and further described in Attachment A-1.
- b. **MICHAEL SELLERS's** black Chevy Tahoe ("TARGET VEHICLE"), Florida temporary registration: CNZ1236, and further described in Attachment A-2.

AGENT BACKGROUND, TRAINING, & EXPERIENCE

2. I am a Special Agent of the Federal Bureau of Investigation ("FBI") United States Department of Justice and have been employed in that capacity since March 2020. I am currently assigned to the Rhode Island Safe Streets Gang Task Force (hereinafter, the "Task Force") and investigate violent street gangs and drug/firearms trafficking organizations operating in and around the State of Rhode Island. Prior to my employment with the FBI, I served in the United States Navy from 2011-2016 and I worked as a Law Enforcement Officer in the City of Norfolk, Virginia from 2016-2020, where I worked in a capacity as a uniformed patrol officer and a Detective investigating violent street crimes in and around the city of Norfolk.

3. I am a “federal law enforcement officer” within the meaning of the Federal Rule of Criminal Procedure 41 (a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. I have received training in the field of narcotics and firearms enforcement and investigations. I am familiar with the habits, methods, routines, practices, and procedures commonly employed by persons engaged in the trafficking of illegal firearms and drugs. I have been the affiant on dozens of affidavits in support of search warrants, arrest warrants, Title III Wiretaps, GPS location warrants and other applications. Through my training, education and experience, I have become familiar with the manner in which illegal narcotics and firearms are transported, stored, and distributed, and with the methods of payments for such items.

5. Additionally, based on my training and experience and my participation in other controlled substance investigations, I know that it is common for drug dealers to “front” (provide on consignment) controlled substances to their customers; conceal contraband, the proceeds of drug sales, and store drugs/firearms and cash in remote locations sometimes referred to as “stash houses;” maintain records of drug and gun transactions; and use cellular telephones to facilitate their illegal distribution operations. I also know that drug/weapons trafficking is an illicit business and an ongoing process requiring the development, use, and protection of a communication network to facilitate daily drug distribution. Drug dealers use various methods to thwart law enforcement detection, including frequently changing cellular phones and vehicles, using various aliases, and uses coded communications. Based on my experience in drug and firearm investigations, I know that traffickers frequently refer to illicit drugs and guns in guarded conversations and frequently use code words when referring to controlled substances or money.

6. Based upon my training and experience and my participation in this investigation, I know that:

a. Drug traffickers often place assets, including apartments, houses, vehicles, and telephones, in names other than their own to avoid detection of these assets by government agencies. Although these assets are held in other names, the drug dealers actually know or use these assets and exercise dominion and control over them. Records relating to these assets are frequently found in their residences and other locations controlled by them.

b. Person involved in drug trafficking conceal in their vehicles, residences, and businesses; controlled substances, large amounts of currency, financial instruments, precious metals, jewelry, and other items of value, and/or proceeds of drug transactions, and evidence of financial transactions relating to obtaining, transferring, secreting, or spending money made from engaging in narcotic trafficking activities. Money, tangible property and records relating to these assets are frequently found in their residences and other locations controlled by them.

c. Drug traffickers often carry, on their person or maintained in secure locations, weapons to protect themselves and their controlled substances from theft by other users, traffickers, or criminals, and from seizure by law enforcement agencies. Drug traffickers store these weapons in their residences, vehicles, and/or businesses and stash houses, or other locations controlled by them.

d. Drug traffickers commonly maintain addresses or telephone numbers in books, papers, computers, cellular telephones and other electronic data storage devices, and other information that reveals the names, addresses, and/or telephone numbers for

their associates in the drug trafficking organization, even if that information may be in code. Records and electronic devices of this sort are frequently found on the persons of drug traffickers or in their residences, motor vehicles, and other locations controlled by them.

e. Drug traffickers frequently take, or cause to be taken, photographs and/or videos of themselves, their associates, or their property. Records in the form of photographs and/or videos are often found in the residences, offices, or other places under the control of drug traffickers, and provide valuable evidence of the conspiratorial relationships. Records of this type are sometimes in hard copy, but are increasingly found stored on computers, cellular telephones, thumb drives, and other items possessing the capability of storing electronic data.

f. Drug traffickers often keep equipment and materials for packaging, cutting, weighing, manufacturing, and distributing controlled substances in their homes, stash houses, or other locations controlled by them. That drug paraphernalia often includes, but is not limited to, scales, plastic wrap, plastic bags, surgical gloves, presses, and cutting agents as well as aromatic substances such as soap, dryer sheets, wood shavings, and heat sealers, which are used to mask the odor of illegal drugs in an attempt to avoid detection by drug detection dogs. Large-scale drug traffickers sometimes use money counting machines to help count and sort the proceeds of drug trafficking.

g. Drug traffickers commonly consign controlled substances and weapons to their clients and couriers. They frequently maintain books, records, receipts, notes, ledgers, airline tickets, money orders, and other papers relating to the transportation, ordering, sale, and distribution of controlled substances. Records of this type are kept in

location where traffickers have ready access to them, including on their person or in their residences, vehicles, businesses, stash houses, and smart telephones, tablets, and personal computers. Drug and gun traffickers also normally maintain these items and records for long periods of times, regardless of whether their value to the dealer has diminished. Oftentimes, this type of evidence is generated, maintained, and then forgotten about. Thus, documents that one would think a prudent person would destroy because of their incriminatory nature are still possessed months or even years after the documents came into the possession of the drug dealer. Oftentimes, these individuals do not even realize the incriminatory nature of the documents they keep. Documentary evidence dating back years is sometimes found in residences and other locations controlled by traffickers.

h. Persons who reside in or who are using a particular residence will often have documents, bills, and correspondence that list their names and addresses in that residence. Documents such as personal telephone books, address books, utility company receipts, keys, personal letters, rent receipts, mortgage documents, clothing, and other articles of personal property would tend to establish residency at a particular location and provide valuable evidence concerning ownership and control over areas in which drugs or other incriminating evidence are found. Records and documents of this type may also be found in hard copy or stored electronically on computers, mobile telephones, and other media that stores data electronically.

BACKGROUND, METHODS & MEANS

7. This investigation was initiated by the FBI Rhode Island Safe Streets Gang Task Force. This affidavit is based on my own investigation and on information reliably provided to me by other federal, state, and local law enforcement agents in Rhode Island. I have relied on

information supplied by Agents, Troopers, Detectives, and Officers from the FBI, Rhode Island State Police, Providence Police Department, Woonsocket Police Department, Central Falls Police Department, West Warwick Police Department, Cranston Police Department, Pawtucket Police Department, and the United States Marshals Service. I have also relied on reports of investigations that I have prepared or that were prepared by other law enforcement agents; business records, and public and/or law enforcement databases. I have also relied on information provided to me and to other law enforcement agents by a Cooperating Witness.

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of the investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in relevant part only.

Cooperating Witness #1

8. A Cooperating Witness (hereinafter, "CW-1") has been providing the FBI with information regarding SELLERS since approximately November 2023. CW-1 has been compensated with monetary payments for his cooperation in this investigation thus far and will continue to be paid for his cooperation in this investigation. CW-1 has a criminal history that includes, theft, breaking and entering, possession of stolen goods, obstruction, narcotics violations, traffic violations, possession of a weapon, and domestic violence offenses. CW-1 has served jail time for breaking and entering, domestic violence, theft, and driving offenses and has been found to be in violation probation. CW-1 is currently on bail for a pending felony

offense. He was recently investigated by law enforcement for theft and was found to be in possession of narcotics and agreed to cooperate with law enforcement. CW-1 was not charged with the possession or theft offense. Since the start of his cooperation, CW-1 has provided me with information that I or other law enforcement agents have independently corroborated through toll records, physical surveillance and other law enforcement confidential sources. CW-1 is willing to testify in this investigation and has communicated with SELLERS by phone calls and text messages in the presence of law enforcement. On each occasion, CW-1 communications with SELLERS were monitored and recorded by myself or another member of law enforcement. CW-1 has participated in controlled purchases of narcotics from SELLERS that were monitored and recorded. CW-1 knows SELLERS as a person from whom he can purchase fentanyl pills and crystal methamphetamine from. Prior to the start of the investigation, CW-1 showed members of law enforcement photos of SELLERS, whom the CW-1 knows as “Mike,” and identified him as a supplier of fentanyl pills. In order to protect CW-1’s identity, I will refer to CW-1 with a masculine pronoun regardless of CW-1’s gender.

Controlled Purchases

9. Over the course of this investigation, CW-1 has participated in two controlled purchases of narcotics from SELLERS. In each case, CW-1 arranged the drug deal by contacting SELLERS at the following cell phone number provided by SELLERS: (401) 447-7503 (“the 7503 number”¹). On each occasion, the contact was by text messages, phone calls, or both, and a quantity of narcotics was ordered. The calls made by CW-1 were recorded and conducted in the presence of myself or another participating law enforcement officer. The text messages sent and

¹ The 7503 number is listed as SELLER’S contact telephone in a Rhode Island Department of Corrections (“RIDOC”) Database as of June 14, 2023. According to the RIDOC database SELLERS was last in RIDOC custody at the Adult Correctional Institution from June 14, 2023, to June 15, 2023.

received by CW-1 were photographed by me or another participating law enforcement officer. On each occasion, law enforcement investigators checked CW-1 for contraband prior to the transaction to be sure that he was not already in possession of any narcotics, and that he did not have any additional cash on his person. CW-1 was then supplied with only enough official government funds for the purchase of the amount of narcotics that had been ordered. In addition, CW-1 was equipped with an audio and video recorder for all controlled buys in which he participated. CW-1 was followed to the transaction sites, and surveillance was maintained near those locations. Following each transaction, CW-1 was followed to a predetermined meeting location where he turned over the narcotic evidence to me or another law enforcement officer working on this investigation. In each case, CW-1 was debriefed, and the audio and video recording devices were retrieved and reviewed. Additionally, a field test was performed on all of the drugs that had been purchased. In every instance, the field tests returned a positive indication for the presumptive presence of the drug that was purchased. Whenever I use the term “controlled purchase” in this affidavit, this is the procedure that we followed.

10. After each controlled purchase, the drugs were secured as evidence and have been submitted to the Drug Enforcement Administration (DEA) Northeast Laboratory.

SUMMARY OF PROBABLE CAUSE TO SEARCH

11. **On Thursday November 16, 2023**, while in my presence and the presence of another member of law enforcement, the CW-1 was instructed to contact SELLERS on the 7503 number and make an order of 1,000 pills of fentanyl laced pills, which the CW-1 believed to be counterfeit based on previous unrecorded conversations with SELLERS in which SELLERS claimed to have made the pills himself.

12. At approximately 11:50 AM, at my direction, the CW-1 made an outgoing call to SELLERS on the 7503 number. During the call, the CW-1 inquired about the price for purchasing a larger quantity of pills from SELLERS. SELLERS told the CW-1 that he could sell the CW-1 pills for \$2.50 a pill and the CW-1 stated he is looking to purchase 1,000 but would call SELLERS back to confirm.

13. At approximately 11:56 AM, at my direction, the CW-1 made an outgoing call to SELLERS on the 7503 number. During the call, the CW-1 confirmed that he wanted to purchase 1,000 pills and confirmed the price of \$2,500 for the pills. SELLERS agreed to the deal and told the CW-1 to meet at the ALDI's parking lot, located on Smith Street. The CW-1 agreed to meet with SELLERS at that location in 30 minutes.

14. I know this location to be 539 Smith Street, Providence, Rhode Island. In anticipation of a controlled purchase taking place at this location, members of law enforcement initiated surveillance at 539 Smith Street.

15. At approximately 12:12 PM, a member of law enforcement and I searched the CW-1's person and vehicle for any narcotics or money with negative results. The CW-1 was provided with two recording devices (equipped with audio and video) and \$2,500 of Official Agency Funds ("OAF"). The CW-1 was instructed to go to 539 Smith Street, Providence, Rhode Island, meet with SELLERS and exchange the \$2,500 of OAF for 1,000 fentanyl pills.

16. At approximately 12:14 PM, the CW-1 departed the pre-determined meeting location and was continuously surveilled by me and another member of law enforcement to 539 Smith Street, where the CW-1 arrived at approximately 12:22 PM.

17. At approximately 12:37 PM, a member of law enforcement observed the TARGET VEHICLE arrive at 539 Smith Street, Providence, Rhode Island, the TARGET

VEHICLE did not have a front plate and had a temporary rear plate registration of CNZ1236².

The members of law enforcement could not confirm the state of the temporary registration.

18. At approximately 12:39 PM, members of law enforcement observed the TARGET VEHICLE park directly behind the CW-1's vehicle and observed a black male exit the TARGET VEHICLE and walk toward the CW-1's passenger side door and enter the side of the vehicle. A member of law enforcement confirmed that the person who exited the TARGET VEHICLE and entered the CW-1's vehicle was SELLERS. It should be noted that prior to the controlled purchase taking place, all members of law enforcement were provided a photograph of SELLERS and are familiar with his physical appearance and physical characteristics.

19. At approximately 12:44 PM, members of law enforcement observed SELLERS exit the CW-1's vehicle and get into the TARGET VEHICLE.

20. At approximately 12:45 PM, the CW-1 was observed by a member of law enforcement departing the area and was surveilled by myself and another member of law enforcement to a pre-determined meeting location where the CW-1 arrived at approximately 12:51 PM.

21. Additionally, at 12:45 PM, a member of law enforcement observed a passenger in the TARGET VEHICLE with SELLERS and observed the TARGET VEHICLE move away from the parking spot and park in front of an Advanced Auto store in the same parking lot as ALDI's where the controlled purchase took place.

² I conducted a national license plate analysis which I believe the license plate to be a temporary license plate from Florida. NCIC database check shows this registration to belong to a SOLD black Cadillac 4D, bearing the VIN: 1G6KF57951U129633, belonging to ANTONIO DINOTA, with an address of 301 Lakeview Drive Apartment 203, Weston, Florida. The check also provided the registrant information to be THOMAS PETER BOUSQUET, DOB: 09/25/1960, with an address of 67 Ivy Avenue, Cranston, Rhode Island.

22. At approximately 12:47 PM, a member of law enforcement observed SELLERS exit from the driver seat of the TARGET VEHICLE and walk into the Advanced Auto. The member of law enforcement also confirmed that the license plate of the TARGET VEHICLE was in fact, CNZ1236 and was a temporary registration. The passenger of the vehicle stayed inside of the TARGET VEHICLE.

23. At approximately 12:51 PM, SELLERS was observed exiting the Advanced Auto by law enforcement and got into the driver seat of the TARGET VEHICLE and departed the location. SELLERS was continuously surveilled by the surveillance team and was observed entering the gas station located at 201 Smith Street, Providence, Rhode Island at 12:57 PM.

24. At approximately 1:04 PM, a member of law enforcement observed the TARGET VEHICLE depart from the gas station and travelled back toward the ALDI's parking lot where he met with the CW-1.

25. SELLERS and the TARGET VEHICLE were continuously surveilled by the surveillance team and where they observed the TARGET VEHICLE take a right onto Huxley Avenue and then pulled into the driveway of the TARGET PREMISES where SELLERS arrived at approximate 1:05 PM.

26. At approximately 1:06 PM, a member of law enforcement observed an unknown female passenger exit the passenger side of the TARGET VEHICLE and walk toward the TARGET PREMISES.

27. At approximately 1:08 PM, a member of law enforcement observed SELLERS exit the front driver's side of the TARGET VEHICLE and walk toward the hood of the TARGET VEHICLE and stand around the hood of the TARGET VEHICLE.

28. At approximately 1:10 PM, at my direction, surveillance was terminated due to the inability to properly sit on the street without being detected by SELLERS.

29. At the pre-determined meeting location with the CW-1, the CW-1 provided to me and the other member of law enforcement, two plastic baggies containing approximately 500 fentanyl pills in each baggie totaling 1,000 pills that were colored pink with "K 56" stamped on them. Based on my training and experience, the pills appear to be counterfeit K 56 oxycodone. Additionally, the CW-1 provided me with the audio/video recording devices and was searched for any remaining narcotics or money with negative results.

30. The CW-1 was debriefed and told members of law enforcement that as the CW-1 arrived at the controlled purchase location, the CW-1 sent a text message to SELLERS at the 7503 number to tell SELLERS that he was there. After a short while, the CW-1 called SELLERS at the 7503 and asked him if he could bring the CW-1 a cigarette. SELLERS told the CW-1 that he would be able to and told the CW-1 that he would be there in 3 minutes. The CW-1 stated when SELLERS arrived, he entered the front passenger seat of the CW-1's vehicle and took the money from the CW-1. SELLERS counted the money and then reached over to his right-side waistband and got the two baggies of pink fentanyl pills and gave them to the CW-1. SELLERS then exited the area and departed the parking lot and drove toward the pre-determined meeting location where the CW-1 met with myself and the other member of law enforcement.

31. A field test was conducted on the suspected fentanyl pills which yielded a positive result for the presence of fentanyl. I weighed the suspected fentanyl pills which had a gross weight of 104.0 grams. Myself and another member of law enforcement packaged and heat-sealed the suspected fentanyl pills and turned the evidence into the FBI Boston evidence room to be submitted to the DEA Northeast Laboratory for further testing.

32. I reviewed the audio and video recorders which identified SELLERS as the person, who entered the CW-1's vehicle and provided the CW-1 with the 1,000 pink fentanyl pills for the \$2,500 of OAF. Additionally, a member of law enforcement took a photograph of SELLERS as he entered the front passenger side of the CW-1's vehicle which also identified SELLERS as the person who entered the CW-1's vehicle.

33. **On Friday, November 24, 2023**, while in my presence and the presence of another member of law enforcement, the CW-1 was instructed to contact SELLERS on the 7503 number and make another order of 1,000 pills of fentanyl laced pills.

34. At approximately 11:40 AM, at my direction, the CW-1, placed a consensually recorded call to the 7503 number. The call was not answered.

35. At approximately 12:56 PM, at my direction the CW-1 sent a text message to SELLERS on the 7503 number stating, *"Hit me as soon as you get this \$\$\$\$\$ on deck."*

36. At approximately 1:10 PM, CW-1 received a text message from SELLERS on the 7503 number stating, *"25 Minutes away."*

37. At approximately 1:34 PM, at my direction the CW-1 placed a consensually recorded outgoing call to SELLERS on the 7503 number, the call was not answered.

38. At approximately 1:36 PM, at my direction, the CW-1 sent another text message to SELLERS on the 7503 number asking, *"Hit me back when can my g"* and *"I need another 1000 but can you go lower the 25 and if you can throw me a sample of Tina to give to my people they fuck with it hard body."* The CW-1 and I know Tina to be a slang term for Crystal Methamphetamine.

39. At approximately 1:47 PM, the CW-1 received an incoming call from SELLERS on the 7503 number, the call was placed on speaker for myself and another member of law

enforcement to listen to and consensually record. Prior to the call, the CW-1 was instructed to order 1,000 pills and get a sample of crystal methamphetamine, additionally the CW-1 attempted to get the pills for a lower price. CW-1 did as instructed, however, SELLERS responded to the CW-1 stating exactly, *"No bullshit, that's me not really eating shit off that [unintelligible] Ill probably make like a dollar on the you know what I am sayin? Off the shit like on some real sh-real real real shit."* At my direction the CW-1 agreed to the price for \$2,500 and agreed to meet at the same location as last time.

40. I know that the location of the last controlled purchase was at the ALDI's on Smith Street, located at 593 Smith Street, Providence, Rhode Island. Additionally, I also know that when SELLERS is stating that he "isn't really eating off that" he is explaining that if he sells the pills for any cheaper then he won't be making any money off the pills, therefore he is selling them at the cheapest he is able to sell them to the CW-1.

41. In anticipation of the controlled purchase taking place at 593 Smith Street, member of law enforcement initiated surveillance at both the ALDI's on Smith Street as well as SELLERS, residence, the TARGET PREMISES.

42. At approximately 2:02 PM, a member of law enforcement and I searched the CW-1's person and vehicle for any narcotics or money with negative results. The CW-1 was provided with two recording devices (equipped with audio and video) and \$2,500 of OAF. The CW-1 was instructed to go to 539 Smith Street, Providence, Rhode Island, meet with SELLERS and exchange the \$2,500 of OAF for 1,000 fentanyl pills.

43. CW-1 was continuously surveilled from the pre-determined meeting location to 539 Smith Street, where he arrived at approximately 2:17 PM.

44. At approximately 2:18 PM, a member of law enforcement observed SELLERS in the parking lot on foot walking toward the CW-1's vehicle and enter the front passenger seat of the CW-1's vehicle. As SELLERS entered the CW-1's vehicle, members of law enforcement observed the vehicle begin to drive away from the parking lot and exit the parking lot taking a right onto Smith Street and initiated surveillance on the CW-1's vehicle.

45. The CW-1 was observed taking a right onto Tydall and then taking a left onto Pasteur Street, crossing over to Huxley Avenue.

46. At approximately 2:22 PM, a member of law enforcement observed the CW-1 park across the street from the TARGET PREMISES while SELLERS remained in the front passenger seat of the CW-1's vehicle.

47. At approximately 2:24 PM, a member of law enforcement observed the front passenger side of the CW-1's vehicle, and myself and other members of law enforcement identified SELLERS as he walked across the street from the CW-1's vehicle toward the TARGET PREMISES. SELLERS was observed walking down the driveway toward the rear of side of the TARGET PREMISES, where there is a back door.

48. At approximately 2:30 PM, the CW-1 reached out to a member of law enforcement and advised him that SELLERS had to go inside the residence to get the pills and crystal methamphetamine.

49. At approximately 2:35 PM, SELLERS was observed walking down the driveway from the TARGET PREMISES toward the CW-1's vehicle and entered the front passenger seat of the CW-1's vehicle and they departed the location. CW-1 was continuously surveilled by members of law enforcement where he and SELLERS arrived back at the ALDI's/Family Dollar parking lot at 2:39 PM.

50. As the CW-1 and SELLERS were sitting in the parking lot, a marked Providence Police Cruiser entered the parking lot and parked in the parking lot in front of the stores.

51. At approximately 2:54 PM, a member of law enforcement observed SELLERS exit the front passenger side of the CW-1's vehicle and the CW-1 drove away and was continuously surveilled by law enforcement until he arrived at the pre-determined meeting location at 3:15 PM.

52. At 3:02 PM, members of law enforcement advised that SELLERS remained standing around the parking lot after the CW-1 left and was picked up by a grey SUV. Members of surveillance attempted to surveil the vehicle but due to traffic conditions during the day, they were unable to, and surveillance was terminated.

53. At the pre-determined meeting location with the CW-1, the CW-1 provided to me and the other member of law enforcement, two plastic baggies containing approximately 500 fentanyl pills in each baggie totaling 1,000 pills that were colored pink with "K 56" stamped on them. Based on my training and experience the pills appear to be counterfeit K 56 oxycodone. The CW-1 also provided me with a small plastic baggie which contained a blue rock-like substance, consistent with the look, feel, and texture of blue colored crystal methamphetamine. Additionally, the CW-1 provided me with the audio/video recording devices and was searched for any remaining narcotics or money with negative results.

54. The CW-1 was debriefed and told law enforcement that as CW-1 arrived at the purchase location, the CW-1 immediately saw and was waived down by SELLERS. SELLERS approached CW-1's vehicle and entered into the passenger seat and directed the CW-1 to take him to his residence and gave him directions to the TARGET PREMISES, where SELLERS told the CW-1 that he had to go inside to get the narcotics. CW-1 stated as SELLERS exited the

vehicle, he walked down the driveway and behind the TARGET PREMISES, where CW-1 explained that he believes there is a door back there. After waiting for a few minutes, SELLERS was observed by the CW-1 walking back down the driveway from the TARGET PREMISES and got into the CW-1's vehicle and drove back to the original meeting location, where SELLERS was going to meet someone else who was supposed to pick him up from the parking lot. While in the ALDI's parking lot, CW-1 explained that he gave SELLERS the \$2,500 of OAF where SELLERS counted it to verify it was the correct amount of money. While he was counting the money, he observed the Providence police officer park in the parking lot and SELLERS didn't want to get out of the vehicle until the police officer left. After counting the money, SELLERS gave the CW-1 the two plastic baggies containing the pills and a separate baggie which contained the blue rock like substance, which the CW-1 believed to be crystal methamphetamine. SELLERS was talking to the CW-1 about the crystal methamphetamine and stated that he does not know what to charge for it and he has a lot of it that was given to him by a girl whose boyfriend had a stash of it but was arrested and he is trying to help her out by selling it. SELLERS described the girl to be someone he met at a social club in Pawtucket, Rhode Island. Once SELLERS exited the vehicle, the CW-1 departed the area and met with myself and the other member of law enforcement at the pre-determined meeting location.

55. A field test was conducted on the suspected fentanyl pills which yielded a positive result for the presence of fentanyl. The suspected crystal methamphetamine also yielded a positive field test result for the presence of methamphetamine.

56. I weighed the suspected fentanyl pills, which had a gross weight of approximately 103.15 grams, and the suspected crystal methamphetamine had a gross weight of approximately 2.1 grams.

57. Myself and another member of law enforcement packaged and heat-sealed the suspected fentanyl pills and crystal methamphetamine and turned the evidence into the FBI Boston Evidence Room to be submitted to the DEA Northeast Laboratory for further testing.

58. I reviewed the audio and video recorders which identified SELLERS as the person, who entered the CW-1's vehicle and provided the CW-1 with the 1,000 pink fentanyl pills and blue crystal methamphetamine for the \$2,500 of OAF.

Digital Devices³ and Request for Biometric Unlocking of Those Devices

59. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

- a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.
- b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as how the device has been used, what it has been used for, who has used it, and who has been

³ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

- c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.
- d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

60. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during execution of a search warrant for a number of reasons, including the following:

- a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

- b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

61. Based upon my involvement and the involvement of other agents in this investigation, I know that drug traffickers regularly communicate using cellular telephones, which has been confirmed in this case through the use of pen registers and toll analysis, some of which is described herein.

62. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- a. I know from my training and experience, as well as information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button

(often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the

data contained within the devices(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user

of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

Conclusion

51. Based on the above, I suggest that there is probable cause to search the people, premises, and vehicle identified in Attachment A-1 through A-2, for the evidence described in Attachment B.



J. Carlos Razon
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed.
R. Crim. P. 4.1 by _____
(specify reliable electronic means)

Date

Judge's signature

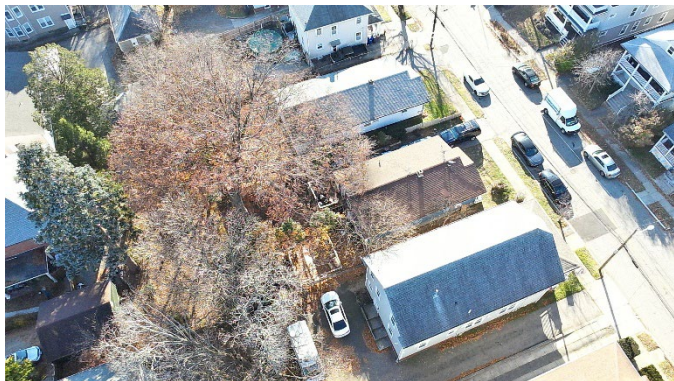
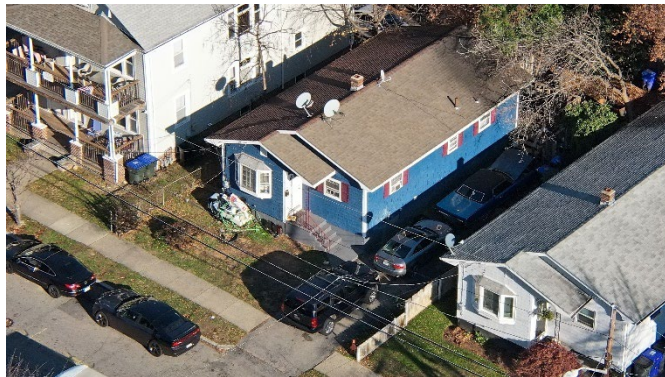
City and State

Printed name and title

Attachment A-1

Premises to be Searched

MICHAEL SELLERS's residence at 47 Huxley Street, Providence, Rhode Island 02920 ("TARGET PREMISES"), described as a 3 bedroom, 2 bathroom ranch. The exterior of the property is painted blue with white accents and red shutters. There is a driveway to the right side of the residence and a front door with a walkway that leads from the driveway. There are 4 stairs that lead up to the front door which is white. To the left of the front door on the door frame is the number "47." There are two mailboxes, however zoning and records show this is a single-family residence. There is a rear door that is white in color. In the backyard there is a wooden raised deck, which leads to the to the rear door. Based on the foundation of the property there also appears to be a basement on the property.



Attachment A-2

Vehicle to be Search

MICHAEL SELLERS's black Chevy Tahoe ("TARGET VEHICLE"), Florida temporary registration: CNZ1236. This registration to belong to a SOLD black Cadillac 4D, bearing the VIN: 1G6KF57951U129633, belonging to ANTONIO DINOTA, with an address of 301 Lakeview Drive Apartment 203, Weston, Florida. The check also provided the registrant information to be THOMAS PETER BOUSQUET, DOB: 09/25/1960, with an address of 67 Ivy Avenue, Cranston, Rhode Island.



ATTACHMENT B

Particular Things to be Seized

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841(a) (1) and 846 (drug trafficking and conspiracy) (herein referred to as the SPECIFIED FEDERAL OFFENSES), namely:

- a) Any controlled substance, controlled substance analogue, or listed chemical;
- b) Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;
- c) Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;
- d) United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;
- e) FINANCIAL RECORDS: All financial records of or relating to MICHAEL SELLERS and his nominees, assignees, or co-conspirators, including but not limited to financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable leases, bank statements, deposit tickets, deposit items, checks, checkbooks, check registers, passbooks, money orders, cashier's checks, official checks,

bank drafts, wire transfer instructions and receipts, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, credit card statements, charge slips, receipts brokerage statements, buy and sell orders and other items evidencing the obtaining, secreting, transfer, or concealment of assets and the obtaining, secreting, transfer, concealment, or expenditure of money;

f) Items showing unexplained wealth or evidencing the proceeds derived from illicit drug trafficking, including but not limited to large sums of money, expensive vehicles, financial instruments, precious metals, jewelry, and real estate, and documents evidencing the procuring or leasing of these items;

g) Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

h) TRAVEL DOCUMENTS: All documents evidencing or relating to foreign or domestic travel of SELLERS; or his co-conspirators, including but not limited to airline tickets, tickets for other means of transport, credit card receipts, travel vouchers, hotel receipts, restaurant receipts, gas receipts, notes, schedules, other receipts evidencing travel, boarding passes, itineraries, luggage tags and receipts, frequent flyer statements and awards, car rental receipts and statements, photographs of travel locations, maps, written directions to a location, visas, passports, United States and foreign customs declaration receipts and forms;

i) Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

j) STORAGE UNIT RECORDS: All records reflecting the ownership or control of storage units including keys, contracts, leases, payments, and inventories;

k) Shipping records, to include any and all receipts (USPS, FedEx, UPS, and DHL) for parcels shipped to SELLERS

l) Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

m) Records, documents, programs, applications or materials, or evidence of the absence of same, including text, instant, and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

n) Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

o) Contents of any calendar or date book;

p) Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

q) Any digital device (SEE BELOW- INCLUDING CELLULAR TELEPHONES AND TABLETS) which itself or which contains evidence, contraband, fruits, or instrumentalities of the SPECIFIED FEDERAL OFFENSES, and forensic copies thereof.

r) Firearms.

s) Keys to a Chevy Tahoe vehicle and to the TARGET PREMISES

described in Attachment A-2.

With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized;

1. evidence of who used, owned, or controlled the digital device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. evidence of software that would allow others to control the cellular phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the lack of such malicious software;
4. evidence indicating how and when the digital device was accessed or used to determine the chronological context of device's access, use, and events relating to the crimes under investigation and to the phone user;
5. evidence indicating the device's user's knowledge and/or intent as it relates to the crimes under investigation;
6. evidence of the attachment to the device of other storage devices or similar containers for electronic evidence;
7. evidence of programs (and associated data) that are designed to eliminate data from the device;
8. evidence of the times the device was used;
9. passwords, encryption keys, and other access devices that may be necessary to access the cellular phone;
10. records of or information about Internet Protocol addresses used by the device and
11. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
12. With respect to any and all electronically stored information in digital devices and cellular devices, in addition to the information described herein, agents may also access, record and seize the following:
 - i. Telephone numbers of incoming/outgoing calls stored in the call registry;
 - ii. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
 - iii. Any incoming/outgoing text messages relating to the above criminal violations;
 - iv. Telephone subscriber information;

- v. The telephone numbers stored in the cellular telephone and/or PDA;
- vi. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
- vii. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular phone/device including but not limited to photographs, videos, e-mail, and voice mail relating to the above SPECIFIED FEDERAL OFFENSES.

As used herein, the terms “records,” “documents,” “programs,” “applications,” and “materials” include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, memory cards, and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

- a. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, “hidden,” or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.